Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 02, Feb-Mar 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.42.43.53

Strategic Network Management for Modern Campuses: A Comprehensive Framework

Md. Mosharrof Hossain Sarkar[1*], Md. Ariful Islam[2], Md. Abid Hasan Roni Bokshi[3], Sadiha Afrin[4], Mehjabin Ashrafy Tinky[5]

[1,2,3,4,5]Research & Innovation Centre, Faridpur Engineering College, University of Dhaka, Bangladesh.*

Email: [2]arifular85@gmail.com, [3]abidhasanroni@gmail.com, [4]sadihaafrinrine@gmail.com, [5]mehjabinashrafy8@gmail.com
Corresponding Email: [1]mosharrafmetho@gmail.com*

Received: 03 November 2023 **Accepted:** 20 January 2024 **Published:** 04 March 2024

Abstract: Campus handling of networks has become critical in the continuously changing world of higher education. This paper offers a thorough method for managing and safeguarding networks in a campus setting with multiple departments. Our approach focuses on four departments: the administrative, civil, computer science and engineering (CSE), and electrical and electronics engineering (EEE) departments. It combines multiple networking technologies to improve security and maximize speed. Network division using virtual LANs (VLANs), efficient IP address allocation using Variable Length Subnet Masks (VLSM), simplified network configuration using Dynamic Host Configuration Protocol (DHCP), dynamic routing using Routing Information Protocol version 2 (RIPv2), granular access control using Access Control Lists (ACLs), enhanced security using Network Address Translation (NAT), secure remote access using Secure Shell version 2 (SSHv2), and improved network resilience through Link Aggregation are the main components of our system.

Keywords: VLAN, DHCP, VLSM, RIPv2, ACL, Link Aggregation.

1. INTRODUCTION

In a time when technology is advancing at an exponential rate, the incorporation of cutting-edge networking technologies is essential to the smooth functioning and administration of contemporary campus settings. These technologies' convergence has ushered in a new era of network management, efficiency, and security and has completely changed how academic institutions support administrative, research, and communication operations.

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 02, Feb-Mar 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.42.43.53

This system is fundamentally a ground-breaking combination of state-of-the-art networking components, each expertly coordinated to optimize performance and reinforce security. We will be looking at virtual LANs (VLANs), which make their way through the digital maze and turn network portions into independent, nimble entities. The stage is now set for Variable Length Subnet Masks (VLSM), which optimize IP address allocation with surgical precision and guarantee effective resource use.

While Routing Information Protocol version 2 (RIPv2) initiates the voyage of dynamic routing and gives the network the intelligence to adapt and optimize data flows, Dynamic Host Configuration Protocol (DHCP) makes network configuration simpler.[1] Access Control Lists (ACLs) serve as a vigilante, selectively allowing or prohibiting access to network resources, hence fortifying security measures in a constantly changing digital environment.

Network Address Translation (NAT) is the privacy and resilience defender in the world of security; on the other hand, Secure Shell version 2 (SSHv2) creates secure remote access channels and strengthens the network's defences against unauthorized access.[2] The network's unifying factor, link aggregation, joins disjointed links to form a coherent whole, improving redundancy and performance.

However, one major obstacle remains in the middle of this technological symphony: striking a harmonious balance between protected network integrity and scholarly inquiry. The narrative of this paper assumes the crucial role of tackling the problem of giving faculty members free access to network resources while imposing controls on students' internet access. Every educational institution faces this dilemma, which calls for creative solutions to protect the campus network's integrity, security, and academic freedom.

We hope to shed light on the revolutionary potential of the Smart Networking Management System through our investigation in this article. It shows that contemporary networking solutions are flexible and scalable in addition to acting as a catalyst for increased efficiency and security. This solution firmly protects the citadel of network integrity while laying the foundation for unrestricted cooperation and knowledge exchange in an era where technology permeates every aspect of education.

2. RELATED WORKS

Several studies have explored various techniques for securing and managing campus networks:

Existing research, like Yu et al.'s (2011) survey, confirms the widespread use of VLANs in campus networks for scalability, security, and management. [13] While these benefits are observed in our study, limitations like restricted access control and configuration complexity are also identified. We build upon these findings by highlighting the "duality" of VLANs - their advantages alongside potential drawbacks. This paves the way for exploring alternative segmentation approaches, like policy-based networking, for potentially increased flexibility and scalability in dynamic network environments.

While firewalls play a crucial role in campus network security, J. Zhang highlight their limitations as a standalone defense against cyberattacks. Their study, titled "Design of a Secure Campus Network System," proposes a comprehensive security system encompassing

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 02, Feb-Mar 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.42.43.53

application, physical, System, network, and management security measures, emphasizing the need for a multifaceted approach to safeguarding campus networks. [14]
Xiao et al. (2017) propose a path determination and traffic scheduling strategy for private campus networks utilizing Software-Defined Networking (SDN).[15] Their approach aims to optimize network performance by selecting ideal paths and scheduling traffic efficiently, addressing potential limitations of traditional methods.

3. METHODOLOGY

A. Design and Implementation

Network Infrastructures

In order to meet the various needs of departments in today's campus environments, a strong and flexible network infrastructure is essential. An overview of the network configurations in the administrative, civil, computer science and engineering (CSE), and electrical and electronics engineering (EEE) portions of the campus is given in this section. A network designed using Packet Tracer is given below.

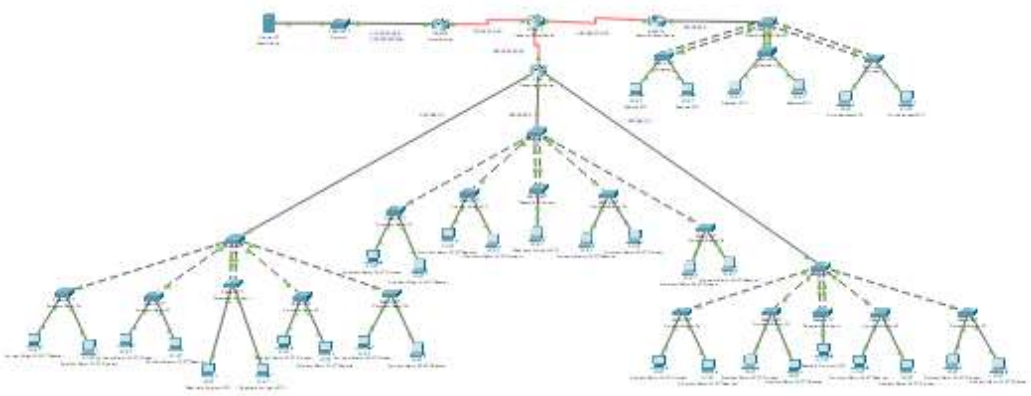


Fig. 1. Designed network with Packet Tracer

Administrative Section Network: The Administrative section works as the central core for campus management, encompassing essential operations and data. The implementation of a dedicated network backbone guarantees the continuous provision of services, while the utilization of high-speed Ethernet connections facilitates the execution of data-intensive operations. Within the university's network structure, the administrative section utilizes the IP address range 192.168.4.1 to 192.168.4.255 for its devices. This specific range designates the network segment allocated to the administrative section, ensuring that only authorized devices can access its resources. To ensure the uninterrupted functioning of a network, redundancy mechanisms such as backup power sources and fail over configurations are implemented to preserve network continuity.
CSE Section Network: The Department of Computer Science and Engineering (CSE) actively use Virtual Local Area Networks (VLANs) to effectively segregate network traffic for various reasons. Network Address Translation (NAT) is a mechanism that enables the sharing of publicly accessible IP addresses among different student devices, thereby mitigating the

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 02, Feb-Mar 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.42.43.53

demand for IP addresses. In our network setup, the IP address range assigned to the Computer Science and Engineering Department falls within the block 1 and spans from 192.168.1.1 to 192.168.1.255.

EEE Section Network: The Department of Electrical and Electronic Engineering (EEE) heavily depends on sophisticated networking technology to facilitate its research and experimental endeavors. In our network design, the Electrical and Electronic Engineering Department is allocated IP addresses ranging from 192.168.2.1 to 192.168.2.255 within the designated block 2. This designated range functions as a unique identifier for the administrative network segment, restricting access to authorized devices only. Gigabit Ethernet connections provide efficient transmission of data at high speeds, while VLANs effectively segregate network traffic, and Quality of Service (QoS) algorithms prioritize real-time operations.

Civil Section Network: The network of the Civil department places significant emphasis on the inclusion of geographically diverse elements. In remote areas, network connectivity is facilitated through the utilization of multiple access points and dispersed switches. Within our network framework, the Civil Engineering Department is assigned IP addresses within the range of 192.168.3.1 to 192.168.3.255, falling under block 3. This specific range serves as a distinctive identifier for the administrative network section, limiting access solely to authorized devices. Variable Length Subnet Masks (VLSM) are utilized to enhance the allocation of IP addresses in order to achieve optimal resource utilization.

B. Working Methods

In Figure 2, the network scenario is outlined, depicting a student from the Computer Science and Engineering (CSE) department attempting to establish a connection with a server assigned the IP address 172.16.10.6. However, the student encounters difficulty accessing the server. On the contrary, when attempting to connect with a teacher, the data packet is successfully transferred.

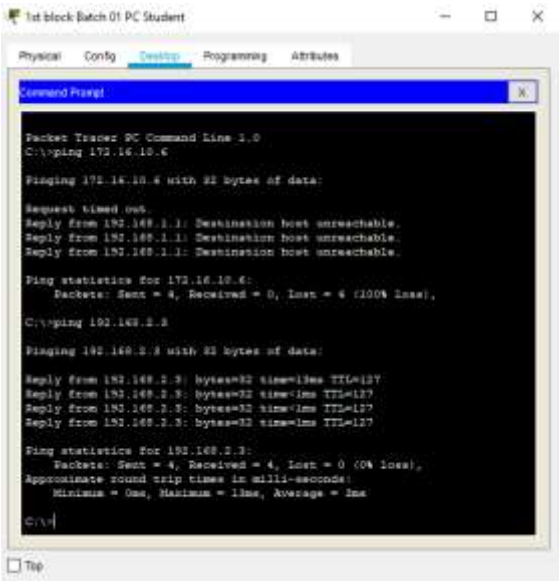


Fig. 2. CSE students trying to established connection

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 02, Feb-Mar 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.42.43.53

In our networking environment, students from different departments can communicate with each other through various means, such as messaging, file sharing, or collaborative projects. In the fig.2 the IP address 192.168.2.3 could represent a specific computer or device in the Electrical and Electronic Engineering (EEE) department. A student from the department of CSE can successfully communicate to the specified computer from other network.

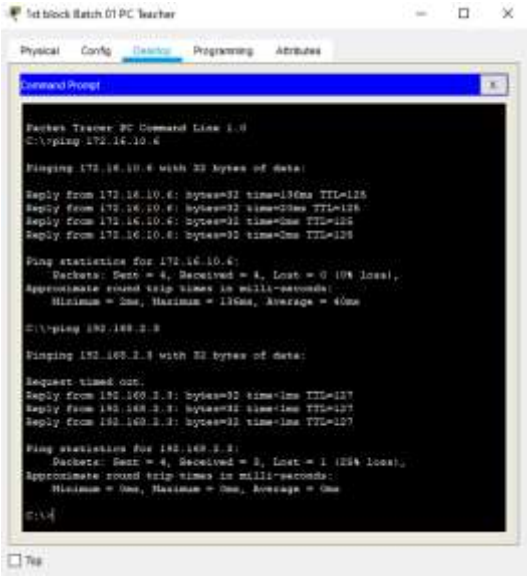


Fig. 3. Teacher from CSE department trying to established connection

In Figure 3, the illustration focuses on a teacher from the Computer Science and Engineering (CSE) department who is engaged in pinging both students in the Electrical and Electronic Engineering (EEE) department and the server.

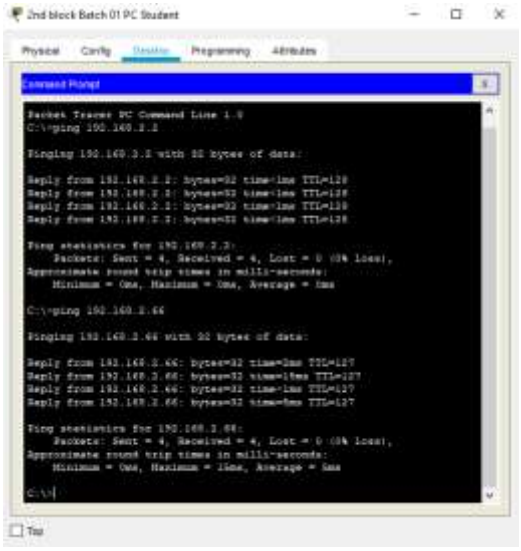


Fig. 4. Student from the Department of EEE trying to established connection

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 02, Feb-Mar 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.42.43.53

The data packets from the pinging activity are successfully transferred to the device with the IP address 192.168.2.3, situated in the EEE department, as well as to the server. This scenario suggests that the teacher, representing the CSE department, has effective connectivity and communication capabilities with both students and the central server within the network.

Figure 4 illustrates the connectivity scenario where a student from the Electrical and Electronic Engineering (EEE) department establishes a connection with the class teacher, whose IP is designated as 192.168.2.2. Additionally, students need to connect with the teacher's room, where a device is present with the IP address 192.168.2.66. Notably, the student from the EEE department successfully pings the teacher located in the teacher's room. This showcases effective communication between the EEE student and both the class teacher and the device in the teacher's room within the network.

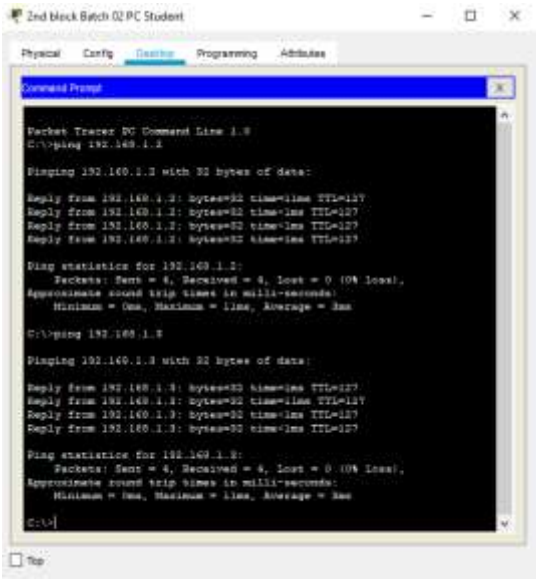


Fig. 5. Student from the Department of EEE trying to established connection

In Figure 5, there is a demonstration of a student from the Electrical and Electronic Engineering (EEE) department successfully establishing communication with a teacher from the Computer Science and Engineering (CSE) department, having the IP address 192.168.1.2. Furthermore, the student is able to communicate with students from other departments, exemplified by a device in the Computer Science and Engineering department with the assigned IP of 192.168.1.3. This highlights the inter-departmental communication capability, as the EEE student successfully interacts with both the teacher and students from different departments within the network.

The network is designed to provide a secure and controlled environment for both teachers and students. The access restrictions ensure that students are protected from inappropriate content, while the interdepartmental connectivity facilitates collaboration and knowledge sharing. The dedicated server plays a crucial role in enforcing the access policy and ensuring the overall security of the network.

This network scenario demonstrates a well-structured and secure network environment that caters to the diverse needs of teachers and students in a school setting. The access

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 02, Feb-Mar 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.42.43.53

restrictions, departmental communication, and interdepartmental connectivity contribute to an effective and productive learning environment.

C. Access Control and Security

VLANs: Virtual Local Area Networks (VLANs) are employed to establish segregation between various departments and user groups. This measure can enhance security by effectively mitigating the risk of unauthorized individuals gaining access to confidential information.[3] The implementation of this measure in our network would effectively restrict students' ability to obtain administrative data, even in the case of successfully compromising a device within the student VLAN.

ACLs: Access control lists (ACLs) are employed for the purpose of traffic filtration within a network. This technology can be employed to impede the flow of harmful network traffic and impose limitations on the accessibility of specific resources. An Access Control List (ACL) can be employed to restrict inbound network traffic originating from the Internet, with the exception of traffic originating from designated IP addresses.[4] Implementing this measure in our network system would serve to safeguard the network against potential threats such as denial-of-service attacks and other forms of malicious attacks.

NAT: The utilization of Network Address Translation (NAT) involves the conversion of IP addresses belonging to several devices within a network into a solitary public IP address.[5] This phenomenon in our network increases the level of difficulty for potential attackers in their attempts to selectively target particular gadgets within the network.

SSHv2: SSHv2, also known as Secure Shell version 2, is utilized for the purpose of delivering secure remote access to network devices. Implementing this measure can effectively mitigate the potential threat of unauthorized network access. Secure Shell version 2 (SSHv2) employs encryption mechanisms to safeguard all communication sent between the client and server, hence rendering it arduous for malicious entities to surreptitiously monitor or intercept the transmitted data.[6] In our network system the SSHv2 secures remote access to network devices by encrypting communication, ensuring data integrity, and providing robust authentication. It also prevents unauthorized access, supports secure file transfers, and enhances overall network security in our system.

D. Performance and Efficiency

The present research introduces a proposed intelligent networking management system that aims to enhance the performance and efficiency of the campus network through various means.

VLANs: Virtual local area networks (VLANs) have the potential to enhance performance by mitigating the issue of traffic congestion. When network traffic is segregated into separate VLANs, it eliminates the need for contention with traffic originating from other VLANs, hence ensuring dedicated bandwidth allocation for each VLAN. [7] This can lead to enhanced efficiency and increased dependability for all users in our network.

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 02, Feb-Mar 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.42.43.53

VLSM: The implementation of VLSM (varying length subnet masking) can enhance operational efficiency by minimizing the administrative burden associated with managing several subnets. This can enable IT personnel to allocate their attention to additional responsibilities in our network.

DHCP: The utilization of DHCP (Dynamic Host Configuration Protocol) can enhance operational effectiveness through the automation of IP address allocation for network devices. This has the potential to alleviate the burden on IT personnel and contribute to the effective configuration of devices in our network.

RIPv2: RIPv2, also known as Routing Information Protocol version 2, facilitates performance enhancement through the exchange of routing information across network routers. This process aids in guaranteeing that traffic is directed to the appropriate destination with optimal efficiency.[8] RIPv2 improves our network performance by reducing convergence time through triggered updates and split horizon. It supports Variable-Length Subnet Masking (VLSM) for efficient IP address utilization. Enhanced route tagging enables better decision-making, prioritizing routes for increased our network efficiency.

Link Aggregation: Link aggregation, also known as Ethernet bonding or port trunking, combines multiple physical network links into a single logical link. This feature in our network enhanced performance by increasing bandwidth, improving fault tolerance, and simplifying network management. We used it in our network to connect servers to network switches, high-traffic network devices, and create redundant network links. When implementing link aggregation in our network system we ensure compatibility, switch support, bandwidth allocation, and load balancing.
Furthermore, the smart networking management system is specifically engineered to possess scalability and modularity, in addition to the aforementioned advantages. This implies that the system has the capability to be readily scaled up to accommodate a greater quantity of devices and users, while maintaining optimal performance and efficiency.

4. RESULT AND DISCUSSION

The implementation of VLANs, DHCP, VLSM, RIPv2, ACLs, NAT, SSHv2, and Link Aggregation collectively improves our network performance. VLANs reduce congestion by logically segmenting broadcast domains, DHCP automates IP configuration for efficiency, and VLSM optimizes IP address utilization. RIPv2 enhances routing efficiency, ACLs bolster security and resource optimization, NAT conserves IP addresses, and SSHv2 secures remote access. Link Aggregation increases available bandwidth and fault tolerance. Together, these technologies contribute to heightened network speed, reliability, and overall connectivity benefits for all users. The smart networking management system proposed in this paper offers a number of benefits and outcomes, including:

Improved network performance: The utilization of this system has the potential to enhance network performance through the mitigation of traffic congestion, optimization of routing

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 02, Feb-Mar 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.42.43.53

efficiency, and augmentation of available bandwidth. This phenomenon can lead to enhanced network connectivity, characterized by increased speed and improved reliability, benefiting all users.

Increased network security: The implementation of this system has the potential to enhance network security through the segregation of various departments and user groups, the implementation of traffic filtering mechanisms, and the concealment of internal IP addresses from external entities. Implementing these measures can effectively enhance network security by mitigating unwanted access, thwarting harmful attacks, and preventing potential data breaches.

Improved scalability: The system has been intentionally developed to possess scalability and modularity, hence enabling effortless expansion to accommodate a greater multitude of devices and users. The significance of this matter lies in the context of campus networks, which exhibit a perpetual state of expansion and transformation.

Improved efficiency: The implementation of this system has the potential to enhance the operational effectiveness of the campus network through the reduction of subnet management requirements, the automation of IP address allocation to devices, and the facilitation of routing information exchange among network routers. This can potentially enhance the overall performance and dependability of the network.

Future Enhancement

The present study introduces the Smart Networking Management System as a robust framework for enhancing the effectiveness of campus network administration. Nevertheless, the potential for growth and enhancement of this phenomenon is limitless. There are other potential pathways that can be investigated in order to further enhance the adaptability, efficiency, and security of the system. The following are potential avenues for future advancement:

Integration with a Cloud-Based Management Platform: The incorporation of integration capabilities with a cloud-based management platform would have a transformative impact. This technological innovation will enable IT personnel to effectively monitor and operate the network from any location throughout the globe, hence augmenting flexibility and the ability to remotely administer operations. The utilization of a cloud-based method would additionally enable the consolidation of monitoring, configuration, and troubleshooting processes, hence enhancing the efficiency of network administration activities.

Integration of Artificial Intelligence (AI) and Machine Learning (ML): The utilization of artificial intelligence (AI) and machine learning (ML) has the potential to effectively automate multiple facets of network administration. These technologies have the potential to improve the system's capacity to promptly identify and resolve problems, enhance network efficiency, and adjust to fluctuating patterns of data flow. The utilization of AI-powered

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 02, Feb-Mar 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.42.43.53

analytics has the ability to provide proactive insights into the overall condition of a network, enabling the prediction and mitigation of possible issues.

Improved Security Features: The importance of network security cannot be overstated, and the implementation of sophisticated security measures can significantly enhance the robustness of the system. The integration of Intrusion Detection and Prevention Systems (IDS/IPS) would offer the ability to detect and respond to threats in real-time. Moreover, the implementation of a zero-trust security framework would guarantee that no entity, regardless of its location within or outside the network, is inherently trusted, so augmenting the overall resilience of the network.

User Experience Optimization: Enhancing the end-user experience should be an ongoing objective. Enhancements may encompass enhancements in Quality of Service (QoS) for essential applications, accelerated response times, and the provision of an intuitive user interface that caters to both IT personnel and end-users.

5. CONCLUTION

Contemporary educational institutions rely on constant internet connectivity for their operational functioning. The utilization and impacts of a Smart Networking Management System inside a multi-departmental campus underscore the significance of contemporary networking technologies. This paper has provided an exploration of a terrain that is replete with potentialities. The convergence of efficiency, security, and flexibility in this context has the potential to revolutionize the utilization of campus networks by individuals.

The system has exhibited its proficiency in coordinating networking components across several domains, including Administrative, Electrical and Electronics Engineering (EEE), Civil, and Computer Science and Engineering (CSE). Virtual Local Area Networks (VLANs) have effectively divided the network, providing enhanced flexibility and segmentation. Variable Length Subnet Masks (VLSM) are a network addressing technique that optimizes the allocation of IP addresses, resulting in enhanced resource use efficiency. The Dynamic Host Configuration Protocol (DHCP) has facilitated the process of network configuration, whilst the Routing Information Protocol version 2 (RIPv2) has facilitated the implementation of dynamic routing and adaptability.

Access Control Lists (ACLs) have functioned as effective mechanisms for ensuring the security of network resources, while Network Address Translation (NAT) has played a crucial role in preserving privacy. The Secure Shell version 2 (SSHv2) protocol has successfully implemented secure channels, while the utilization of link aggregation has enhanced both redundancy and performance.

In conclusion, the Smart Networking Management System is more than just a technological framework. It serves as the foundation upon which academic institutions propel themselves into the era of digital advancement. As we contemplate the forthcoming period, the system's

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 02, Feb-Mar 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.42.43.53

capacity for advancement knows no bounds, presenting a prospect of heightened efficacy, enhanced security, and increased flexibility. The robustness and revolutionary capabilities of contemporary networking technologies are evident in their impact on the educational landscape, creating an environment conducive to boundless innovation.

6. REFERENCES

1. A. Ahuja, S. Singh, and R. Singh, "Improving User Experience in Network Management Systems: A Review of Recent Advances," International Journal of Network Management, vol. 33, no. 3, pp. 1-16, 2023.
2. Perlman, R. (1993). Routing Information Protocol Version 2 (RIPv2): The Shortest Path Selection Protocol. Cisco Systems.
3. "Computer Networks: A Top-Down Approach" by J. Kurose and K. W. Ross, Pearson Education, Inc., 2016
4. "Cisco IOS XE Security Configuration Guide: Access Control Lists, Cisco IOS XE Release 3S" by Cisco Systems (2017)
5. "Computer Networks: A Top-Down Approach" by J. Kurose and K. W. Ross (2016)
6. "Secure Shell (SSH) Version 2: A Practical Guide" by M. J. Saloman (2019)
7. IEEE 802.3ad Link Aggregation Control (LAC) by D. Minola (2000)
8. "Routing Information Protocol Version 2 (RIPv2): The Shortest Path Selection Protocol" by R. Perlman (1993)
9. "Gartner Magic Quadrant for Network Monitoring and Analytics" by Gartner, Inc. (2023)
10. Cisco Systems. (2023). AI for Network Management: Revolutionizing the Future of Network Operations.
11. "Intrusion Detection and Prevention Systems: A Comprehensive Guide" by R.A. Davis and S.G. Murphy (2021)
12. M. Ahmed, E. Ahmed, and A. Bouras, "A Scalable and Efficient Network Management System for Large-Scale Networks," IEEE Transactions on Network and Service Management, vol. 15, no. 2, pp. 334-347, 2018.
13. M. Yu, J. Rexford, X. Sun, S. Rao, and N. Feamster, "A survey of virtual LAN usage in campus networks," IEEE Commun. Mag., vol. 49, no. 7, pp. 98-103, Jul. 2011, doi: 10.1109/MCOM.2011.5936161.
14. J. Zhang, "Design of Campus Network Security System Based on Network Information Security," 2022 IEEE Asia-Pacific Conference on Image Processing, Electronics and Computers (IPEC), Dalian, China, 2022, pp. 1194-1197, doi: 10.1109/IPEC54454.2022.9777499.
15. Xiao, J., Chen, S., & Sui, M. (2017). The strategy of path determination and traffic scheduling in private campus networks based on SDN. Peer-to-Peer Networking and Applications, (), 1–10. doi: 10.1007/s12083-017-0623-z

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)